UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,982	07/12/2000	John R. Hind	5577-199	2459

20792 7590 01/27/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/614,982	HIND ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-38,40-57 and 77* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 8/6/04 have been fully considered but they are not persuasive.

2. In response to applicant's argument that Bealkowski does not teach for a latch to control read and write operations of a programmable memory, the examiner disagrees. A latch can be defined as a single memory cell used in the formation of RAM (see included "Memory System Design"). In the invention taught by Bealkowski, "Stage II Post (RAM based, see Fig 4, element 110) sets a protection means for preventing access to the disk partition holding the BIOS image" (Col 8, Line 13-14). Onelook Online Dictionary defines access, "noun: (computer science) the operation of reading or writing stored information." The system that performs the access prevention can be defined as a memory controller.

3. In response to applicant's argument that Holtley and Davis do not teach that access to a programmable memory is based on the state of a latch, the examiner disagrees. Both Davis and Holtley teach using a computer with RAM latches to protect programmable memory (Col 3, Line 23, '986) (Fig 2, Element 10-4, '424).

4. In response to applicant's argument that Davis does not teach controlling access to a programmable memory, the examiner disagrees. Davis teaches for write access of

a BIOS update to be performed based on the result of a Boolean validation assessment (Fig 3, Element 160, '986)

5. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, knowledge generally available to one of ordinary skill in the art.

6. In response to applicant's argument that Davis does not teach controlling access to the memory where the update control program resides, the examiner disagrees. Davis teaches for the cryptographic coprocessor which validates/controls access to the BIOS memory (Col 2, Line 61, '986) retrieves instructions from the BIOS (Fig 2, Element 60, '986).

7. In response to applicant's arguments stating that Davis does not teach the use of update rules, as broadly as stated in the claims, the digital signature validity check and revision date validity check (Col 4, Line 11, '986) constitute update rules. Starting on Col 4, Line 1, Davis teaches "using the well-known techniques of digital signatures and certificates to validate the integrity and validity of the 'new BIOS program'". Davis further teaches on Col 4, Line 13, "If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used."

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 22 and 27 rejected under 35 U.S.C. 102(b) as being preceded by Bealkowski et al., US Patent No. 5022077 (hereafter referred to as '077).

3. As to claim 22:

'077 teaches a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) comprising:

Latch/latch enable circuit/memory controller allows write access to programmable memory after hardware reset / In response to a reset signal the protection means permits access to the protected region (Col 3, Line 26, '077)

Latch/latch enable circuit/memory controller prevents write access to programmable memory upon completion of memory update window / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image (Col 3, Line 31 et seq., '077)

4. As to claim 27:

Latch/latch enable circuit/memory controller allows read access to programmable memory after hardware reset / In response to a reset signal the protection means permits access to the protected region (Col 3, Line 26, '077)

Latch/latch enable circuit/memory controller prevents read access to programmable memory upon completion of memory update window / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image (Col 3, Line 31 et seq., '077)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-21, 40-57, and 77 rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, US Patent NO. 5844986(hereafter referred to as '986) in view of '424.

7. As to claims 2 and 40:

'986 teaches a method for providing secure BIOS firmware updates comprising:

- Allowing access to programmable memory based on access latch / If the new BIOS is valid... the previous BIOS program is deleted (Col 4, Line 14, '986). It is inherent that the validity variable used in '986 is stored in a memory latch, because this is the way by which computers process information.
- Setting the access latch to allow access after a hardware reset / All BIOS functions take place after a hardware reset

- Executing an update control program (UCP) / Cryptographic Coprocessor performs authentication, validation (Col 2, Line 61, '986), and BIOS replacement (Col 3, Line 49, '986) operations.
- Resetting the latch to prevent access upon completion of the UCP / the validity variable is used only with the BIOS replacement operation.

. '986 does not teach to only allow access to the programmable memory during an update window of authorized access. '424 teaches several security strategies to protect access to a programmable memory, including the use of an authorized access window of predefined duration (Col 5, Line 55, '424). It would have been obvious to a person of ordinary skill in the art at the time of invention employ the security strategies of '424 with the secure BIOS update system of '986. One of ordinary skill in the art would have been motivated to employ the security strategies of '424 with the secure BIOS update system of '986 because utilizing additional security strategies helps to reduce potential security vulnerabilities.

8. As to claims 3 and 41:

Allowing/Preventing access to a memory where the update control program resides based on access latch / If the new BIOS is valid... the previous BIOS program is deleted (Col 4, Line 14, '986). It is inherent that the validity variable used in '986 is stored in a memory latch, because this is the way by which computers process information. Cryptographic coprocessor contains the BIOS firmware (Col 2, Line 59,'986)

9. As to claims 4, 6, 42, and 44:

Determine if an update is available (based on status information) / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Update programmable memory if update is available / the new BIOS is stored internally (Col. 3, Line 58, '986), New BIOS program is made operational (Col 4, Line 14, '986)

10. As to claims 5 and 43:

Determining step examines local memory, local drive, network drive, or input device status / Crypto-coprocessor actively retrieves it from a specified source (eg. system memory) (Col. 3, Line 56, '986), Users download upgrade via Internet (Col 3, Line 43, '986)

11. As to claims 7 and 45:

Obtaining an update image / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Obtaining installation information from update image / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

Writing update data to programmable memory / The new BIOS program is stored internally (Col. 3, Line 58, '986)

12. As to claims 8 and 46:

'986 as modified above teaches a method for providing secure BIOS system driver updates assisted by a BIOS management utility software. '986 does not specifically teach for the BIOS management utility software to be obtained via download. The examiner takes official notice as to obtain the BIOS management utility software with BIOS upgrade via download. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain the BIOS management utility software with BIOS upgrade via download. One of ordinary skill in the art would have been motivated to obtain the BIOS management utility software with BIOS upgrade via download because it is customary to make Internet upgrades available with an installation program. Examples include Microsoft Windows upgrades and peripheral device driver upgrades, etc.

13. As to claims 9 and 47:

Loading update image temp workspace / First storage element for storing a code update, a second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

14. As to claims 10 and 48:

Storing existing data to provide a backup copy / A second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

15. As to claims 11 and 49:

Determining if the update was successful, restoring use of the backup copy/ If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

16. As to claims 12 and 50:

Verifying the authenticity of the update / Cryptographic coprocessor performs the appropriate authentication operations on the new BIOS program (Col. 3, Line 61, '986)

17. As to claims 13 and 51:

Evaluate at least one certificate... valid digital signature / Using the well known techniques of digital signatures and certificates to validate the integrity and validity of the new BIOS program (Col. 4, Line 1, '986)

18. As to claims 14 and 52:

Decrypt the digital signature using a shared secret / authentication can be preformed... by the use of secret information (Col. 3, Line 65, '986)

19. As to claims 15 and 53:

Decrypting a digital signature using a public key... comparing with precomputed value / public/private key cryptography... using techniques of digital signatures (Col. 3, Line 67, '986)

20. As to claims 16 and 54:

Public key is stored in a non-updateable memory / Cryptographic coprocessor will be preloaded with the public key (Col 4, Line 31, '986)

21. As to claims 17 and 55:

Provide public key in previous versions... obtain public key from programmable memory / Cryptographic coprocessor may be preloaded with another public key that may be used to authenticate a certificate chain to obtain this industry association public key (Col 4, Line 34 et seq., '986)

22. As to claims 18 and 19:

Hierarchical plurality of certificates / certificate chain (Col 4, Line 36, '986)

23. As to claims 20 and 56:

Obtaining/evaluating application rules information from certificate associated with update / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

24. As to claim 21:

Evaluating at least one of rules information associated with a manufacturer of the device, brand of device, software version of the device, license authorization of the device or individual device / revision date (Col 4, Line 11, '986)

25. As to claims 57:

Evaluating rules information associated with one of: manufacturer of the device ... / Certificate associated with manufacturer (Col 2, Line 49, '986)

26. As to claims 77:

Claim 77 corresponds to claim 2.

27. Claims 23, 24, and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of Christeson et al., US Patent No. 5579522 (hereafter referred to as '522).

28. As to claim 23:

'077 teaches a hardware implementation (Fig 2) of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) upon completion of the memory access window started at reset. '077 does not teach a read only memory containing a program associated with a processor to update the programmable memory. '522 teaches the use of a read only recovery BIOS with recovery update functionality for updating a corrupted system BIOS (Col 6, Line 30 et seq., '522) . It would have been obvious to a person of ordinary skill in the art at the time of invention to use the recovery BIOS with

recovery update feature of '522 in addition to the protected BIOS system in '077. One of ordinary skill in the art would have been motivated to use the recovery BIOS with recovery update feature of '522 in addition to the protected BIOS system in '077 because doing so would protect the system of '077 from being inoperable in the event that the system BIOS has been corrupted.

29. As to claim 24:

Executing the program contained in the read only memory upon generation of the hardware reset / Upon power up or reset, the processor jumps to a location within the protected recovery BIOS block (Col 3, Line 18, '522)

30. As to claim 25:

Set the latch to the second state upon completion of execution of the program / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image. Bios then boots the operating system (Col 3, Line 31 et seq., '077). It would be necessary to prevent access to the newly updated system BIOS to ensure the further protection upon completion of the recovery BIOS/update and transfer of system control to the operating system.

31. Claim 26 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of '522 in further view of "Introduction to Digital Signal Processors" (hereafter referred to as DSP).

32. As to claim 26:

'077 as modified above teaches hardware implementation (Fig 2) of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) utilizing a 80386 PC processor. Not specifically taught is for the processor to comprise a digital signal processor. DSP teaches a Pentium PC processor with MMX. It would be obvious to a person of ordinary skill in the art to use the more modern Pentium processor with MMX in place of the 80386 exemplified in '077. One of ordinary skill in the art would have been motivated to the more modern Pentium processor with MMX in place of the 80386 exemplified in '077 because the Pentium MMX series of processors provides similar functionality and greater speed to that of the 80386.

33. Claims 28-38 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of '986.

34. As to claims 28 and 30:

'077 teaches a hardware implementation of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) upon completion of the memory access window started at reset. '077 does not teach to determine (based on status information) if a BIOS update is available then update the BIOS. '986 teaches a method for actively receiving and securely updating BIOS firmware. It would have been obvious to a person of ordinary

skill in the art at the time of invention to use the BIOS updating means of '986 with the BIOS protection means of '077. One of ordinary skill in the art would have been motivated to use the BIOS updating means of '986 with the BIOS protection means of '077 because field updating of BIOS firmware can help to correct programming errors or corrupted copies of the existing BIOS.

35. As to claim 29:

Determine if an update is available by examining local memory, local drive, network drive, or input device status / Crypto-coprocessor actively retrieves it from a specified source (eg. system memory) (Col. 3, Line 56, '986), Users download upgrade via Internet (Col 3, Line 43, '986)

36. As to claim 31:

Obtaining an update image / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Obtaining installation information from update image / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

Writing update data to programmable memory / The new BIOS program is stored internally (Col. 3, Line 58, '986)

37. As to claim 32:

BIOS updating means of '986 with the BIOS protection means of '077

'077 as modified above teaches a BIOS protection means providing secure BIOS system driver updates assisted by a BIOS management utility software. '077 as modified above not specifically teach for the BIOS management utility software to be obtained via download. The examiner takes official notice as to obtain the BIOS management utility software with BIOS upgrade via download. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain the BIOS management utility software with BIOS upgrade via download. One of ordinary skill in the art would have been motivated to obtain the BIOS management utility software with BIOS upgrade via download because it is customary to make Internet upgrades available with an installation program. Examples include Microsoft Windows upgrades and peripheral device driver upgrades, etc.

38. As to claim 33:

Loading update image temp workspace / First storage element for storing a code update, a second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

39. As to claim 34:

Storing existing data to provide a backup copy / A second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

40. As to claim 35:

Determining if the update was successful, restoring use of the backup copy / If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

41. As to claim 36:

program is configured to verify the authenticity for the update of the programmable memory if an update of the programmable memory is available / Cryptographic coprocessor performs the appropriate authentication operations on the new BIOS program (Col. 3, Line 61, '986)

As to claim 37:

Program is configured to obtain application rules information from an extension of at least one certificate associate with the update, evaluate the rules information obtained form a certificate and selectively update the programmable memory based on the evaluation of the rules information obtained from the certificate / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986), revision date validity check (Col 4, Line 11, '986)

As to claim(s) 38:

Obtain application rules from update image, evaluate obtained rules, update programmable memory based on evaluation / Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986), revision date validity check (Col 4, Line 11, '986)

Conclusion

42. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

43. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306

44. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100